

(19)



JAPANESE PATENT OFFICE

## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002182769 A**(43) Date of publication of application: **26.06.02**

(51) Int. Cl.

**G06F 1/00**  
**G06F 12/14**  
**G11B 20/10**

(21) Application number: **2000383123**(71) Applicant: **HITACHI LTD**(22) Date of filing: **12.12.00**(72) Inventor: **NAGATANI TAKESHI**

(54) **SOFTWARE AUTHENTICATING METHOD  
 UTILIZING CARTRIDGE**

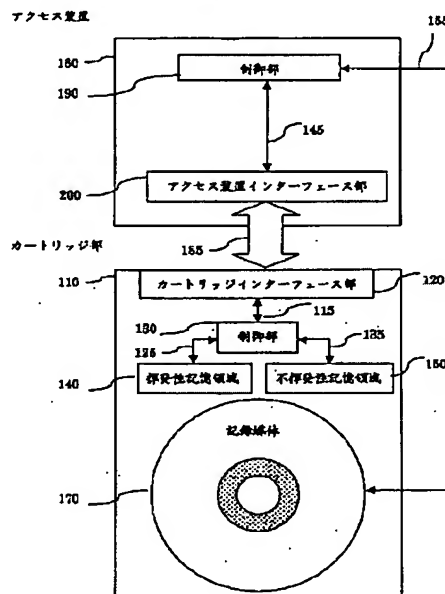
COPYRIGHT: (C)2002,JPO

図 3

(57) Abstract:

**PROBLEM TO BE SOLVED:** To provide a system and a method for suppressing an illegal use of software license.

**SOLUTION:** The controlling part 190 of an accessing device 180 requests the controlling part 130 of a cartridge 110 to perform a software installation authentication in the case of installing software stored on a recording medium 170 inserted into the cartridge 110. The controlling part 130 authenticates the software based on authentication algorithm stored in a nonvolatile storage area 150, stores information proper to the type of machine in a volatile storage area 140 when this authentication is successful and allows the software to be installed. In the case of uninstalling the software, the controlling part 190 of the accessing device 180 requests uninstallation authentication in the same manner as the installation authentication, and the controlling part 130 allows the software to be uninstalled when the uninstallation authentication successful and erases the information proper to the type of machine stored in the storage area 140.



BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-182769  
(P2002-182769A)

(43) 公開日 平成14年6月26日 (2002.6.26)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)
G 0 6 F 1/00		G 0 6 F 12/14	3 2 0 A 5 B 0 1 7
	12/14	G 1 1 B 20/10	H 5 B 0 7 6
G 1 1 B 20/10	3 2 0	G 0 6 F 9/06	6 6 0 D 5 D 0 4 4

審査請求 未請求 請求項の数 4 O L (全 6 頁)

(21) 出願番号 特願2000-383123 (P2000-383123)

(22) 出願日 平成12年12月12日 (2000. 12. 12)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 永谷 剛

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

(74) 代理人 100075096

弁理士 作田 康夫

Fターム(参考) 5B017 AA03 BA05 BB03 CA15

5B076 FB06

5D044 BC03 BC06 CC04 DE49 DE50

GK17 HL08

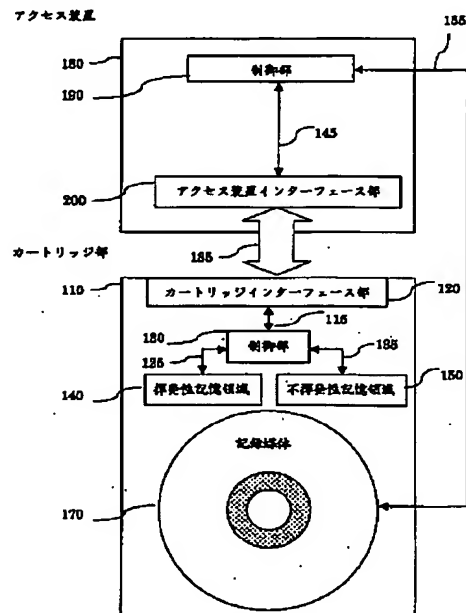
(54) 【発明の名称】 カートリッジを利用したソフトウェア認証方法

(57) 【要約】

【課題】 ハードウェア及びソフトウェアの組み合わせで着脱可能な記録媒体に格納されたソフトウェアの不正インストール防止。

【解決手段】 カートリッジ110に装着された記録媒体170に格納されたソフトウェアのインストールの際、アクセス装置180の制御部190はカートリッジ110の制御部130に対しソフトウェアのインストール認証要求を行う。制御部130は不揮発性記憶領域150に格納された認証アルゴリズムに基づきソフトウェアの認証を行い、成功時に揮発性記憶領域140に機種固有情報を格納してインストールを許可する。ソフトウェアのアンインストールの際アクセス装置180の制御部190はインストール時と同様アンインストール認証要求を行い、成功すれば制御部130がアンインストールを許可し、揮発性記憶領域140に格納された機種固有情報を消去する。

図 3



**【特許請求の範囲】**

**【請求項 1】** 揮発性記憶領域と不揮発性記憶領域が内蔵されたカートリッジに着脱可能な記録媒体を挿入して、カートリッジ内の不揮発性記憶領域に格納された認証アルゴリズムと、ソフトウェアのインストールプログラムと、ソフトウェアをインストールするシステム装置固有のシステム情報と、記録媒体が持つソフトウェア固有の情報と、カートリッジアクセス装置を利用する事を特徴とするソフトウェアコピーガード実現方法。

**【請求項 2】** システム装置にアプリケーションをインストールする際、カートリッジ内の不揮発性記憶領域に格納された認証アルゴリズムによる演算結果を揮発性記憶領域に格納されたソフトウェアのライセンス情報に反映する事を特徴とするソフトウェアの不正利用防止方法。

**【請求項 3】** システム装置内にインストールされた対応アプリケーションを完全に消去する際、カートリッジ内の不揮発性記憶領域に格納された認証アルゴリズムによる演算結果を揮発性記憶領域に格納されたソフトウェアのライセンス情報に反映する事を特徴とするソフトウェア不正利用防止方法。

**【請求項 4】** 請求項 2 と請求項 3 の機能を利用して、着脱可能な記録媒体に格納されたソフトウェアをユーザが所持するライセンス数より多いシステム装置へのインストールを防止する特徴を持つソフトウェア不正利用防止方法。

**【発明の詳細な説明】****【0001】**

**【発明の属する技術分野】** 本発明は、ソフトウェアの不正利用の防止およびソフトウェアのユーザライセンス管理を行う為に使用する認証方法、着脱可能な記録媒体および装置の技術に関する。

**【0002】**

**【従来の技術】** 一般的なパーソナルコンピュータでは、ソフトウェアのインストール時にソフトウェアに付属するソフトウェアの ID キーを入力、またはソフトウェアが書き込まれている記録媒体自身にソフトウェア的な処理を施す事によって、ソフトウェアの不正インストール等の防止を行っている。また、ソフトウェアのインストール時にライセンス数の情報等をシステム装置のディスク装置等へ書き込む手段等でソフトウェアのライセンス管理を行っていた。

**【0003】**

**【発明が解決しようとする課題】** 従来の技術だけでは事前にインストールするソフトウェアの ID キーを入手、または記録媒体そのものを複製する手段があれば、不正な方法で入手したソフトウェアでも通常にインストールして利用する事が出来るといった問題があった。また、ソフトウェアのライセンスの管理情報に関してもディスク装置等へ書き込む事によるライセンス情報を管理する

方法の場合、不正なプログラム等を利用してライセンス管理情報を意図的に改変し、許諾されたライセンス数より多い数のシステム装置で不正利用するケースが考えられる。

**【0004】** 本発明は、上記の実情を踏まえてソフトウェアのライセンス不正利用を抑止するシステムおよび方法を提供する事を目的とする。

**【0005】**

**【課題を解決するための手段】** 課題を解決する為に、アクセス装置の他に複製が難易な不揮発性記憶領域を内蔵したカートリッジを新しく設け、本不揮発性記憶領域内にソフトウェア認証アルゴリズムおよび認証キーを格納し、これらを利用していないとソフトウェアのインストールを不可能にする仕組みを持つソフトウェアの認証を行う。

**【0006】**

**【発明の実施の形態】** 以下、本発明の実施の形態について図面を参照して説明する。

**【0007】** 最初に、認証に必要な各ハードウェアの発明のハードウェア的な実施形態を図 1、図 2、及び図 3 を用いて説明する。

**【0008】** 図 1 はシステム装置にインストールするソフトウェアを格納した記憶媒体 170 と記録媒体 170 内のソフトウェアを認証する為の中心になるカートリッジ 110 を表している。

**【0009】** カートリッジ 170 は着脱可能な記録媒体 170 を格納する記録媒体装着部 160 と、記録媒体 170 に格納されたソフトウェアをシステム装置にインストールまたはアンインストールする際に実行する認証アルゴリズムと認証アルゴリズムに使用する認証キーの両方を格納した不揮発性記憶領域 150 と、対象ソフトウェアをインストールした際に生成される演算結果を格納する揮発性記憶領域 140 と、認証アルゴリズムの処理および揮発性記憶領域 140 と不揮発記憶領域 150 を I/O コントロールに関する処理を行う制御部 130 と、後述するカートリッジを読み取るアクセス装置との情報のやり取りを行うカートリッジインターフェース部 120 から構成される。

**【0010】** 記録媒体 170 をカートリッジ 110 の記録媒体装着部 160 に格納した状態を示すのが図 2 である。

**【0011】** 認証アルゴリズムはカートリッジ 110 の不揮発性記憶領域 150 に格納されている為、記憶媒体 170 に格納されたソフトウェアの認証方法を変更するには、現在使用しているカートリッジ 110 を別の認証アルゴリズムを不揮発性記憶領域 150 に格納したカートリッジ 110 と差し替える事によって実現する事が可能である。

**【0012】** カートリッジ 110 の不揮発性記憶領域 150 に格納する認証アルゴリズムは同じ入力情報に対し

て必ず同じ演算結果を出力し、異なる入力データに対しては必ず異なる演算結果を出力する必要がある。

【0013】実際にソフトウェアのインストールとアンインストールを行う際には図2の記録媒体170が格納された状態のカートリッジ110の他に、カートリッジ110とソフトウェアの認証に必用なデータ等をやりとりする為のインターフェース部とカートリッジ110の中に格納された記録媒体170にアクセスする機能を持つアクセス装置180が必用である。

【0014】着脱可能な記録媒体170に格納されたソフトウェアのインストール、またはアンインストールを行う際、記録媒体170をカートリッジ110の記録媒体装着部160に挿入した後に、記録媒体170が装着されたカートリッジ110をアクセス装置180に装着する。

【0015】ソフトウェアのインストール時の認証処理における発明の処理形態を図3および図4を参照して説明する。

【0016】ソフトウェアのインストールの際（ステップS101）には、アクセス装置180の制御部190はアクセス装置インターフェース部200とカートリッジ110のカートリッジインターフェース部120を経て、カートリッジ110の制御部130に対してインストール認証処理を要求する。

【0017】インストール認証処理の要求により、カートリッジ110の制御部130は不揮発性記憶領域150に格納された認証キーと、ソフトウェアをインストールするシステム装置の固有情報、および記録媒体170の中に格納されたソフトウェア識別キーを取り出して、不揮発性記憶領域150内に格納された認証アルゴリズムに従って演算（ステップS102）を行い、その演算結果を揮発性記憶領域140内に格納されている演算結果のリストと比較して同じ演算結果がリストに存在するか確認（ステップS103）する。

【0018】カートリッジ110の制御部130は、前記の演算結果（ステップS102）が既に揮発性記憶領域140内に格納されていた場合は、ソフトウェアのインストール認証の結果を成功とし、アクセス装置180の制御部190に対しソフトウェアインストール処理の続行を許可（ステップS106）する。

【0019】カートリッジ110の制御部130は、前記の演算結果（ステップS102）が揮発性記憶領域140内に存在していない状態で、かつ揮発性記憶領域140内に演算結果を格納するための領域が残っている場合（ステップS104）は、演算した結果（ステップS102）を揮発性記憶領域140にライセンス情報として格納した後に（ステップS105）、ソフトウェアのインストール認証の結果を成功と判断し、アクセス装置180の制御部190に対して、ソフトウェアインストール処理の続行を許可（ステップS106）する。

【0020】カートリッジ110の揮発性記憶領域140に書き込む事が可能な演算結果（ステップS105）の領域の上限はインストールするソフトウェアによって許諾されているライセンス数までとする。

【0021】上記の理由の為、カートリッジ110の制御部130は、前記の演算結果（ステップS102）が揮発性記憶領域140内に存在していない状態で、かつ揮発性記憶領域140内に演算結果を格納するための領域が残っていない場合（ステップS104）は、ソフトウェアのインストール認証の結果を失敗と判断して、アクセス装置180の制御部190に対しソフトウェアインストール処理の続行を中断（ステップS107）させる。

【0022】あるシステム装置にインストールされたソフトウェアのライセンスを他のシステム装置で利用する等の理由で未使用状態にするには、カートリッジ110の揮発性記憶領域140内にソフトウェアのライセンス情報として格納されている演算結果を消去する必要がある。この場合、ライセンスを手放すシステム装置の情報が格納されたカートリッジ110と、アクセス装置180と、対象となるソフトウェアの記録媒体170を利用して対象ソフトウェアをアンインストールする必用がある。

【0023】ソフトウェアのアンインストール時の認証処理における発明の処理形態を図3および図5を参照して説明する。この処理を利用する事でソフトウェアがインストールが許諾されたライセンス数を超えない事を保証する。

【0024】アンインストール認証処理の要求（ステップS201）に対しては、カートリッジ110の制御部130は不揮発性記憶領域150に格納された認証キーとソフトウェアをアンインストールするシステム装置の固有情報、および記録媒体170に格納されたソフトウェア識別キーを取り出して、不揮発性記憶領域150内に格納された認証アルゴリズムに従って演算（ステップS202）を行い、導き出された演算結果を揮発性記憶領域140内に格納されている演算結果のリストと比較して同じ演算結果が存在するか確認（ステップS203）する。

【0025】カートリッジ110の制御部130は、前記の演算結果（ステップS202）が揮発性記憶領域140内に既に存在している場合は、ソフトウェアのアンインストール認証の結果を成功とし、アクセス装置180の制御部190に対しソフトウェアのアンインストール処理の続行を許可（ステップS204）する。そして、ソフトウェアのアンインストール終了後に、導き出した演算結果と同じ内容を揮発性記憶領域140に格納された演算結果のリストから消去（ステップS206）する。

【0026】カートリッジ110の制御部130は、前

記の演算結果（ステップS202）が揮発性記憶領域140内に存在していない場合は、ソフトウェアのアンインストール認証の結果を失敗として、アクセス装置180の制御部190に対しソフトウェアのアンインストールの処理を中断（ステップS205）する。

#### 【0027】

【発明の効果】着脱可能な記録媒体内の従来のバイナリ情報を変更する事なく、ソフトウェア利用の抑制およびユーザに許諾されたソフトウェア利用ライセンスの管理を実現する。

【0028】着脱可能な記録媒体の既存の標準規格との互換性を保持しつつ、ソフトウェアへの対応および利用ソフトウェアのライセンス管理を行うことが可能である。

【0029】本発明はさらに不揮発性記憶領域内のバイナリ情報を変更する事により着脱可能な記録媒体のバイナリ情報を変更する事なく、必用に応じて認証方法を変更する事が可能である。

【0030】本発明はカートリッジ内の認証アルゴリズムを利用する事により媒体を特定のシステム装置以外で利用不可能にする事が可能である。

【0031】本発明はカートリッジ内の複製不可能な不揮発性記憶領域に認証アルゴリズムを格納されており、かつ揮発性記憶領域にソフトウェアのライセンス情報を格納する為、着脱可能な記録媒体を複製された場合でもソフトウェアの不正利用を抑制する事が可能である。

#### 【図面の簡単な説明】

【図1】着脱可能な記録媒体をカートリッジに挿入する図。

【図2】着脱可能な記録媒体がカートリッジに装着された状態を示す図。

【図3】アクセス装置、着脱可能な記録媒体とカートリッジ間のインターフェース及びデータの流れを示す図。

【図4】着脱可能な記録媒体からソフトウェアをインストールする際の認証処理の流れを示す図。

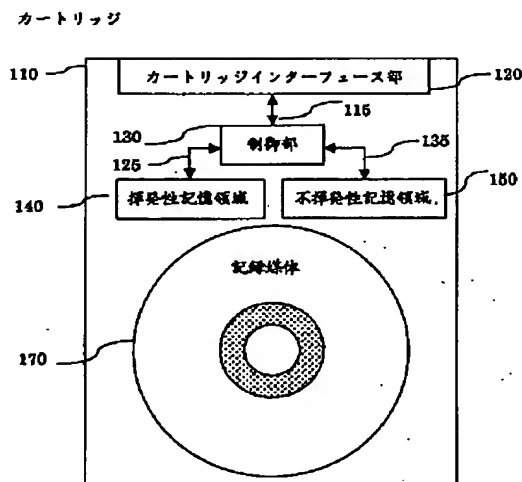
【図5】システム装置からソフトウェアをアンインストールする際の認証処理の流れを示す図。

#### 【符号の説明】

110…カートリッジ、115…カートリッジインターフェース部と制御部のバス、120…カートリッジインターフェース部、125…カートリッジ制御部と揮発性記憶領域のバス、130…カートリッジ内の処理制御部、135…カートリッジ制御部と不揮発性記憶領域のバス、140…カートリッジ内揮発性記憶領域、145…アクセス装置の制御部とアクセス装置のバス、150…カートリッジ内不揮発性記憶領域、155…アクセス装置の制御部と着脱可能な記録媒体、160…着脱可能な記録媒体の装着部、170…着脱可能な記録媒体、180…アクセス装置、190…アクセス装置制御部、200…アクセス装置側のカートリッジ媒体へのインターフェース。

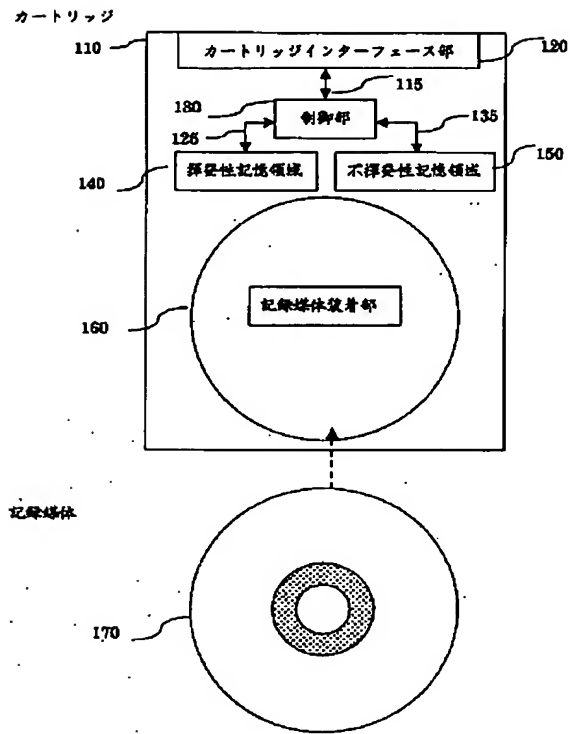
【図2】

図 2



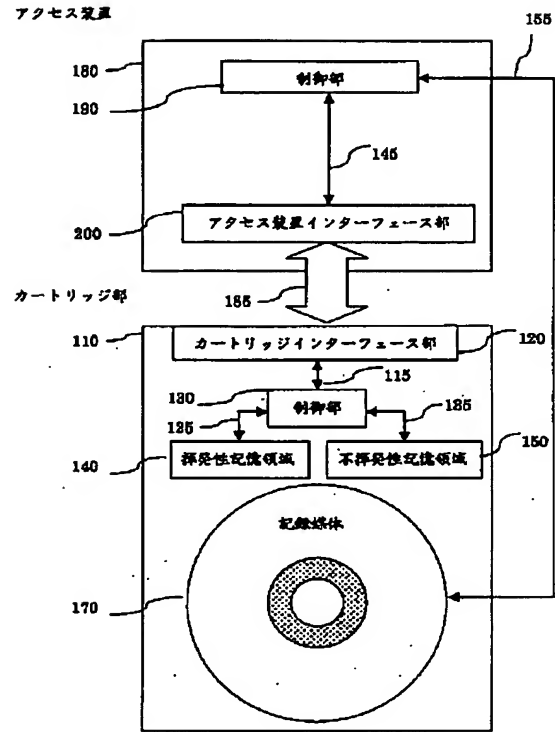
【図1】

図 1



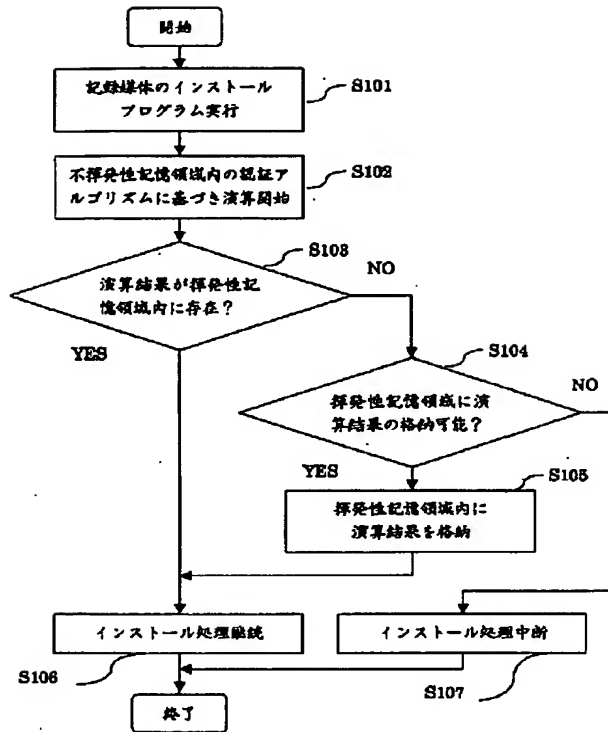
【図3】

図 3



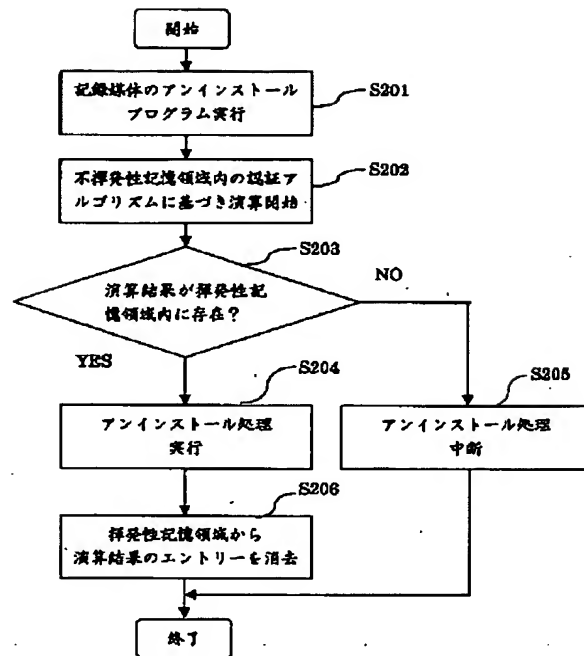
【図4】

図 4



【図5】

図 5



This Page is inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLORED OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REPERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images  
problems checked, please do not report the  
problems to the IFW Image Problem Mailbox**